谷山・志村予想(Fermat予想)に関するWilesの仕事の概略について

AUTHOR(S):

栗原, 将人

CITATION:

栗原, 将人. 谷山・志村予想(Fermat予想)に関するWilesの仕事の概略について. 代数幾何学シンポジューム記録 1993, 1993: 161-181

ISSUE DATE:

1993

URL:

http://hdl.handle.net/2433/214596

代数幾何学シンポジウム記録
1993年度 pp.161-181

谷山・志村予想（Fermat予想）に関するWilesの仕事の概略について

都立大・理　栗原将人

これを書いている現在（主催者の好意に甘えて1ヶ月程締め切りを遅らせてもらい1994年1月中旬にこれを書いているのだが）Wilesの Fermat予想に関する仕事については あの部分にgapがあった，いやこの部分にもgapがある，などと尾鰭を噂がいろいろと飛んでいる。当初1993年9月に発表になると言われていた論文も未だ発表にならない。Wiles自身が去年の12月に発表したコメントは次の通りである。

自分の証明を詳しく吟味していく中でいくつもの問題点が明らかになってきた。そのうちのほとんどは解決できたのだが 特にそのうちの1つを未だ解決できないでいる。谷山志村予想（のほとんどの場合）を Selmer群の計算に帰着する という重要なstepは正しい。しかしながら（保型形式に作う表現のsymmetric squareに関する）semi-stableな場合のSelmer群の位数を正しい値で上から押さえる という最後の計算が現状ではまだ完全でない。しかしCambridgeで説明したようなAのアイディアで近いうちにこの部分も完成できると私は信じている。

これ以上現時点での状況を書いたとしてもこの報告集が出る頃には歴史的興味しか残らないだろう。そこで上の文章の中にある Selmer群の位数の計算に帰着するとはどういうことか，そしてその計算はどうなされるのか，というポイントをふまえつつ 現在の自分の知識の範囲内で解説していこうと思う。筆者の力と知識が不十分なため 不満足な解説とならざるを得ないことをおわびし

ます。ところで講演の題名では谷山・Weil予想としたのだが、ここ数ヶ月の間にこの名称は改められつつあり、将来は谷山志村予想として定着しそうなので、ここでも上のように題名を改めさせて頂いた。

§1. 谷山・志村予想 $\Longrightarrow$ Fermat予想

1.1. Serre予想

代数体のGalois表現については Langlands 哲学などがあるが、有理数体の絶対Galois群の有限体上2次の表現については次のようなSerre予想とよばれる詳しい予想がある。

$\mathbb{F}_q$ を標数が p の有限体, $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ とする。

Conjecture 1.1.1 (Serre [S])

$$\rho : G_{\mathbb{Q}} \longrightarrow GL_2(\overline{\mathbb{F}}_q)$$

を絶対既約, odd (c を複素共役としたとき $\det \rho(c) = -1$) なるGalois表現とする。このとき ρ から2つの正の整数 N, k を決める方法があって (この方法 cf. [S] については ここでは詳しく述べるが), ρ は重さ k, level N ($\Gamma_0(N)$), の modular form に伴う表現から得られる。

ここでは重さ k, level N の modular form に伴う表現から得られる, とは次のような意味である。f が重さ k level N の modular form であるとは f は上半平面 H 上の正則関数でしかも "cusp でも正則", さらに

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \pmod{N} \right\} \text{ に対して}$$

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

をみたすということである。modular forms の空間には Hecke 作用素なる作用素たちが定義される。f は cusp-form (各 cusp で消える) で Hecke 作用素の eigen form に

な，っているとする。$F=\sum_{n=1}^{\infty} A_n q^n \quad q=e^{2\pi i z} \quad A_1=1$
a とき（各 A_n は代数的数で）

$\rho_F : G_{\mathbb{Q}} \longrightarrow GL_2(K) \qquad [K:\mathbb{Q}_p]<\infty$

なる表現で Np a 外で不分岐，すべての $\ell \nmid Np$ なる ℓ に対し $\mathrm{tr}\,\rho_F(\mathrm{Frob}_\ell)=A_\ell$ （Frob_ℓ は ℓ で a Frobenius）なるそのを構成できる．（Kuga-Sato variety を使って etale cohomology で作る（Deligne））$\mathcal{O}_K$ を整数環，m を極大 ideal とする。適当な lattice をとり ρ_F を $G_{\mathbb{Q}} \longrightarrow GL_2(\mathcal{O}_K)$ と考え さらに reduction mod m したもの $G_{\mathbb{Q}} \longrightarrow GL_2(\mathcal{O}_K/m)$ が modular form に付う表現から来るもの a 意味である。

Remark 1.1.2. N は Serre では p と素な数として定義される。（p を除いて $\mathfrak{C}$ a Artin conductor）しかし以下では level Np a modular form から来る表現，などと使うことがある。（Serre a 定義で level N, 重さ $p+1$ を level Np 重さ 2 と考えることがある。）

Fermat 予想はこの Serre 予想から従う。

Conjecture 1.1.3. (Fermat) $a^p+b^p=c^p$ をみたす正の整数 a, b, c は p が 3 以上の素数のとき存在しない。

Fermat が Diophantus に書き込みをしたのは何故か 1637 年（寛永 14 年）と言われている。少なくとも息子の Samuel が書き込みスミの Diophantus を出版した 1670 年以前（もちろんそれより，た 1665 年以前とも言える）であることはまちがいない。特にこの時代にはほとんど記号注えなく Fermat は上の Fermat 予想を式として書くことすらできない程の時代に属した人である ということだけ注意しておく。

Weil はその著書 Number Theory a 中で Fermat が扱ったのはほとんど genus 0 か 1 a 曲線に集中しており，彼が

genus 2 以上の曲線をまじめに扱う，たとえば考えるべき，と述べている。しかし上の問題は楕円曲線の問題に帰着されるのである！

Theorem 1.1.4. (Frey, Serre) Serre 予想は Fermat 予想を導く。

証明. $a^p+b^p=c^p$, a, b, c は正の整数，互いに素，$p \geq 5$ とする。このとき

$$E_{Frey}: y^2 = x(x-a^p)(x+b^p)$$

なる楕円曲線を考える。E_{Frey} の p 等分点からできる Galois 表現を

$$\rho_{E_{Frey}}: G_{\mathbb{Q}} \longrightarrow GL_2(\overline{\mathbb{F}}_p)$$

と書くと，$x(x-a^p)(x+b^p)=0$ の判別式が $(abc)^{2p}$ であることから，この表現は $2p$ の外で不分岐，p で crystalline (この場合) = finite = flat = $\mathbb{Z}_p$ 上 finite flat group scheme から来る) となり，ということがわかる。このことから $\rho_{E_{Frey}}$ から計算される Serre の invariant N, k を計算すると $N=k=2$ となる。つまり上の表現は level 2, 重さ 2 の cusp form から来ることになるが，$X_0(2)$ の genus は 0 でありこのような cusp form は存在しない ($H^0(X_0(2), \Omega^1)=0$) ので矛盾。

かくて世の中が Serre 予想のように美しい，という立場に立てばこれで Fermat 予想の証明は終わっている。と言っていては数学にならないので先へ進む。

1.2. Conjecture ε

上の証明では Serre 予想のほんの一部が使われたにすぎない。そこで次のような Serre 予想の一部を考える。

Conjecture 1.2.1. (Conjecture ε in semi-stable, $k=2$)

$\rho: G_{\mathbb{Q}} \to GL_2(\bar{\mathbb{F}}_\ell)$

は level N, 重さ 2 a modular form から得られるとする。N は squarefree で, N を割るある素数 ℓ に対し, $\ell \neq p$ のとき ρ は ℓ で不分岐, $\ell = p$ のとき ρ は ℓ で crystalline (= $\mathbb{Z}_p$ 上 a finite flat group scheme から得られる) とする。このとき ρ は level N/ℓ, 重さ 2 a modular form から得られる。

この予想は Ribet により証明された。証明は level の上げ下げをどうして進めて行くのだが (cf. [R]) ここでは立ち入らない。

Theorem 1.2.2. (Mazur, Ribet) 1.2.1 は正しい。

従って Theorem 1.1.4 の証明が残される。

Corollary 1.2.3. E_{Frey} の conductor を N, $\rho_{E_{Frey}}$ を E_{Frey} の p 等分点 $E_{Frey}[p]$ が作る表現とする。$\rho_{E_{Frey}}$ が重さ 2 level N の modular form に伴う表現から来れば, Fermat 予想は正しい。

1.3. 谷山志村予想

Conjecture 1.3.1. (谷山, 志村) E を有理数体 $\mathbb{Q}$ 上定義された楕円曲線, conductor を N とする。このとき modular curve $X_0(N)$ から non constant な morphism

$\phi: X_0(N) \to E$

が存在する。

従って Theorem 1.2.2. の系として Corollary 1.2.3 は次のようにて書ける。

Corollary 1.3.2. E_{Frey} が谷山志村予想をみたせば，Fermat 予想は正しい。

conductor N が squarefree な楕円曲線（つまり good reduction か multiplicative reduction しか reductions に持たない）を semi-stable な楕円曲線とよぶ。E_{Frey} はこの条件をみたすから

Corollary 1.3.3. semi stable な楕円曲線に対して谷山志村予想が成立すれば Fermat 予想は正しい。

そして Wiles が証明した（と思われる）のはまさにこの主張である。

Theorem 1.3.4.（Wiles） semi stable な楕円曲線に対して谷山志村予想 1.3.1 が成立する。

従って Fermat 予想が成立することになる。以下で述べるのは Theorem 1.3.4. の証明の概略である。

§2. Mazur の deformation 理論についての Wiles の定理

2.1. Mazur 理論（cf. [M]）

$\mathbb{F}_q$ を標数 p の有限体，p は奇素数とする。S を p を含む素数の有限集合とし $G_{\mathbb{Q},S}$ を S に入らぬ素数で不分岐な $\mathbb{Q}$ の代数拡大の最大のものの Galois 群とする。ここに言う Mazur の deformation 理論とはつぎのようなものである。

$$\rho : G_{\mathbb{Q},S} \longrightarrow GL_2(\mathbb{F}_q)$$

を絶対既約な表現とするとき，ρ には universal deformation

が存在する。すなわち $\bar{\rho}$ を剰余体に持つ完備ネーター局所環 R^{univ} と $\rho^{univ}: G_{\mathbb{Q},S} \longrightarrow GL_2(R^{univ})$ で universal なもの（$GL_2(R^{univ})$ の元で mod 極大イデアルで単位元となるものによる共役を除き）一意的に存在する。universal とは R がやはり $\bar{\rho}$ を剰余体に持つ完備ネーター局所環として ρ lifting $G_{\mathbb{Q},S} \longrightarrow GL_2(R)$ が存在するとすると $\varphi: R^{univ} \longrightarrow R$ なる準同型が存在して，この準同型が

$$\begin{array}{ccc} G_{\mathbb{Q},S} & \xrightarrow{\rho^{univ}} & GL_2(R^{univ}) \\ & \searrow & \downarrow \varphi \\ & & GL_2(R) \end{array}$$

なる可換図式を作る，ということである。ここでは Wiles に従って deformation にさらに条件をつけた version で考える。

$\chi: G_{\mathbb{Q}} \longrightarrow \mathbb{Z}_p^{\times}$

で 1 の p 巾乗根 $\mu_{p^\infty} = \bigcup \mu_{p^n}$ への $G_{\mathbb{Q}}$ の作用を表すことにする（cyclotomic character）。$\mathbb{Z}_p$-algebra R に対しても自然な写像 $\mathbb{Z}_p^{\times} \to R^{\times}$ と χ との合成 $G_{\mathbb{Q}} \longrightarrow R^{\times}$ を χ_R，混乱の恐れのないとき，単に χ と書くことにする。Wiles はもう少し一般でやっているのだがここでは次の仮定で話を進める。まず絶対既約な表現 $\rho: G_{\mathbb{Q},S} \longrightarrow GL_2(\bar{\mathbb{F}}_p)$ はさらに次の条件をみたすとする。

2.1.1. $\det \rho = \chi$

2.1.2. ρ は ordinary かまたは flat.

ここに ordinary とは（$\overline{\mathbb{Q}}$ の素点を 1 つとって）D_p を $G_{\mathbb{Q}}$ の p での分解群としたとき，

$\rho|_{D_p} \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$ $\chi_1 \neq \chi_2$, χ_2：不分岐，と書けるということ。flat とはここでは ordinary でなく，$\rho|_{D_p}$ が $\mathbb{Z}_p$ 上の finite flat group scheme から来る，ということであ

とする。さらに deformation にも次の条件をつける。

(D) $\psi: G_{\mathbb{Q},S} \longrightarrow GL_2(R)$ なる ρ の lifting に対して

2.1.3. $\det \psi = \chi_R$

2.1.4. $\rho|_{D_p}$ が ordinary が flat に従い、ψ も ordinary が flat.

2.1.5. R は A-algebra, 環 A については §3.1 で述べる。

ここに ordinary とはやはり $\begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}$, $\psi_1 \neq \psi_2$, ψ_2 は不分岐と書けること, flat とは ordinary でなく すべての finite quotients が finite flat group scheme over $\mathbb{Z}_p$ から来るということ。

以上のような条件をおいてもこの条件の中で universal な ρ の lifting

$\rho_{univ}: G_{\mathbb{Q},S} \longrightarrow GL_2(R_D)$

が存在する (Mazur, Ramakrishna)。

次に modular form に付う表現との関係を見よう。T_D で条件 (D) をおいた universal な Hecke 環を表すとする。このような Hecke 環の存在は ordinary のときも Mazur の deformation 理論の動機となり, 志賀田理論の述べるところである。うつに言うと, level Np^n の modular forms の空間の Hecke 作用素全体がこの空間の自己準同型環の中で生成する可分環(である Hecke 環)の n を走らせたものの逆極限を使って上のような Hecke 環は作られる。(これに条件 D をおこす。) T_D に対応する Galois 表現は Kuga-Sato variety などと言わなくても modular curves の Jacobian の等分点で作れるが, ρ が既約であることから

$\rho_T: G_{\mathbb{Q},S} \longrightarrow GL_2(T_D)$

なる型にできる (T_D は Gorenstein 環になる)。ここで すべての $\ell \notin S$ に対し ρ_T は $Tr(\rho_T(Frob_\ell)) = T_\ell$ (T_ℓ は Hecke 作用素 $\in T_D$) をみたす。この表現は modular forms に付う表現の中で universal なものである。実際 Hecke 環と modular forms の空間との双対から,

$T_{\mathfrak{D}} \to \mathcal{O}$ ($\mathcal{O}$ は A の有限次拡大の DVR) なる環準同型は $\mathcal{O}$ 係数の Hecke 作用素に関する eigenform に対応する。($F = \sum A_n q^n$ なる eigenform に $T_\ell \mapsto A_\ell$ なる環準同型が対応する。) 従って Hecke 作用素に関する eigenform に伴う表現 (ただし eigenform は条件 $(\mathfrak{D})$ をみたす)
$G_{\mathbb{Q},S} \to GL_2(\mathcal{O})$ に対して $T_{\mathfrak{D}} \to \mathcal{O}$ なる環準同型があり

$$\begin{array}{ccc} G_{\mathbb{Q},S} & \xrightarrow{\rho_T} & GL_2(T_{\mathfrak{D}}) \\ & \searrow \swarrow & \downarrow \\ & & GL_2(\mathcal{O}) \end{array}$$

となる。逆に $T_{\mathfrak{D}} \to \mathcal{O}$ があると ρ_T から $G_{\mathbb{Q},S} \to GL_2(\mathcal{O})$ が得られるが これは eigenform に伴う表現に他ならない。この意味で ρ_T は modular forms に伴う表現に関する universal deformation である。

よって $R_{\mathfrak{D}}$ は universal deformation algebra だったから

2.1.6 $R_{\mathfrak{D}} \xrightarrow{\tau} T_{\mathfrak{D}}$

なる環準同型で $\tau \circ \rho_{univ} = \rho_T$ なるものが存在する。
τ は全射であることがわかる。

Conjecture 2.1.7. (Mazur) 2.1.5 の全射 τ は同型である。

これは上に説明したことから (大分うつる説明だけれど, たかが) 次のように言ってもよい。

Conjecture 2.1.8. (Mazur) ρ を 2.1.1, 2.1.2 のような絶対既約な表現, $\mathcal{O}$ を $\mathbb{Z}_p$ 上 finite な DVR として
$\psi: G_{\mathbb{Q},S} \to GL_2(\mathcal{O})$ を 2.1.3, 2.1.4 をみたす ρ の lifting とする。このとき ψ は modular form に伴う表現から来る。

2.2. Wiles の定理

Wiles の示したのはもう少し一般の定理なのだが，ここでは次を紹介する。

Theorem 2.2.1. $\rho: G_{\mathbb{Q},S} \longrightarrow GL_2(\overline{\mathbb{F}}_p)$ を 2.1.1., 2.1.2. をみたす絶対既約な表現とする。さらに
(i) ρ は重さ 2 の modular form に伴う表現から来るとする。
(ii) l を素数，$l \neq p$，l は ρ で不分岐とする。D_l を l での分解群とするとき，$\rho|_{D_l}$ は可約である，とする。
(iii) $\mathrm{Sym}^2\rho$ も絶対既約とする。
(iv) $p=3$ または $p=5$ のとき，ある素数 l が存在して $\#\rho(I_l)$ は p で割り切れるとする。ここに I_l は l での惰性群，$l=p$ ととってもよい。
以上の仮定の下に 2.1.6. の写像 $R_{\mathbb{Q}} \longrightarrow T_{\mathbb{Q}}$ は同型となる。

この定理は semi stable な楕円曲線に対する谷山志村予想を導く。(つまり Theorem 2.2.1 は Theorem 1.3.4 を導く。)このことの証明をここでは紹介する。まず何と言ってもこの Theorem 2.2.1 の条件の中では (i) が一番強い条件である。そこで次の定理から始めよう。

Theorem 2.2.2. $\rho: G_{\mathbb{Q}} \longrightarrow GL_2(\overline{\mathbb{F}}_3)$ を 2.1.1 をみたす既約な表現とする。このとき ρ は Theorem 2.2.1 の条件 (i) をみたす，つまり modular。

この定理は Tunnell の結果から出る。Tunnell は $\psi: G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{C})$ なる既約表現で，$PGL_2(\mathbb{C})$ の中での image が S_4 (4 次対称群) の部分群と同型になり，odd (c を複素共役としたとき $\det\psi(c) = -1$) なものはすべて

重さ1, level $\Gamma_1(N)$ の modular form に付う表現から得られることを示した。$GL_2(\mathbb{F}_3)$ を

$$\Phi: GL_2(\mathbb{F}_3) \hookrightarrow GL_2(\mathbb{Z}[\sqrt{-2}])$$
$$\begin{pmatrix} -1, & 1 \\ -1, & 0 \end{pmatrix} \mapsto \begin{pmatrix} -1, & 1 \\ -1, & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \mapsto \begin{pmatrix} \sqrt{-2}, & 1 \\ 1 & 0 \end{pmatrix}$$

により、と理由こえと、$\bmod (1+\sqrt{-2})$ で trace は変わらない ($\operatorname{tr}\Phi(A) \equiv \operatorname{tr} A \pmod{1+\sqrt{-2}}$)。そこで $\rho: G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_3)$ を Φ により $G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_3) \subset GL_2(\mathbb{Z}[\sqrt{-2}]) \subset GL_2(\mathbb{C})$ と思うと Tunnell の条件をみたすから ($PGL_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$) この表現は重さ1 level $\Gamma_1(N)$ の modular form に付う表現から来る。しかし適当な Eisenstein series をかけることにより重さ1の modular form は $\bmod 1+\sqrt{-2}$ では重さ2の modular form とみなすことができるので、この表現も重さ2の modular form に付う表現から得られる。

以下では表現が重さ2の modular form に付う表現から来るとき、単に modular とよぶことにする。この Theorem 2.2.2 を突破口にして、Theorem 2.2.1 を使ってすべてを modular にしていく、というのが谷山志村予想証明の方針である。

Theorem 2.2.1 を仮定して semistable な楕円曲線に関する谷山志村予想を証明しよう。E を $\mathbb{Q}$ 上に定義された semistable な楕円曲線とする。E の3等分点 $E(\overline{\mathbb{Q}})[3]$ からできる Galois 表現

$$\rho_{E[3]}: G_{\mathbb{Q},S} \longrightarrow GL_2(\mathbb{F}_3)$$

を考える。ここに $S = \{E$ a bad reduction prime $\} \cup \{3\}$ である。(ここでいえとこと注意しておくと E が p で ordinary good reduction を持つか multiplicative reduction を持つとき、$\rho_{E[p]}: G_{\mathbb{Q},S} \longrightarrow GL_2(\mathbb{F}_p)$ ($E(\mathbb{Q})[p]$ からできる表現) は 2.1.2 の意味で ordinary, E が p で supersingular good reduction を持つとき 2.1.2 の意味で flat である。)

i) $\rho_{E[3]}$ が全射のとき.
このとき Theorem 2.2.2 から $\rho_{E[3]}$ は modular, また $\rho_{E[3]}$ は Theorem 2.2.1 の条件をすべてみたす。従って $T_3(E)$ を E のある a Tate module とすると Theorem 2.2.1 から $T_3(E) \otimes \mathbb{Q}_p$ は modular となる。Faltings a isogeny theorem から E は modular curve で parametrize される.

ii) $\rho_{E[3]}$ が可約のとき,
今度は E の 5 等分点による表現 $\rho_{E[5]} : G_{\mathbb{Q},S'} \longrightarrow GL_2(\overline{\mathbb{F}_5})$ $S' = \{\text{bad reduction prime} \cup 15\}$ を考える。$\rho_{E[5]}$ も可約であるとすると E は modular curve $X_0(15)$ の $\mathbb{Q}$-rational point をもつことになるが, $X_0(15)$ の cusp でない $\mathbb{Q}$-rational point はすべてわかっていて, たとえば semi-stable な楕円曲線に対応していることがわかっている。従ってこの場合を考える必要はなく, $\rho_{E[5]}$ は既約であるとしてよい。このとき $\mathbb{Q}$ 上の楕円曲線 E' で
① $\rho_{E'[5]} \simeq \rho_{E[5]}$
② $\rho_{E'[3]}$ は全射
となるようなものが存在する。実際, 5 等分点の構造が $\rho_{E[5]}$ と同型になるような楕円曲線がなす moduli space は genus 0 の curve で, E という $\mathbb{Q}$ 有理点があるから, 無限に $\mathbb{Q}$ 有理点が存在する。この有理点の中に $\rho_{E'[3]}$ が全射となるものが存在することは Hilbert の既約性定理を使って示される。さて上のような E' があると, まず条件①から i) により E' は谷山志村予想をみたす。従って $\rho_{E'[5]} \simeq \rho_{E[5]}$ は modular, ここでもう一度 Theorem 2.2.1 を使って E が modular な楕円曲線 (E が谷山志村予想をみたす) ということがわかる。

Fermat 予想 1.1.3 は $p < 4,000,000$ まで証明されていた。従って Fermat 予想というのは大きな素数に関する statement のような気がしていたが, 上の証明で Wiles

は素数は3と5しか使っていないのである！

§3. Selmer 群

3.1. Theorem 2.2.1. の証明

Theorem 2.2.1 は Selmer群に関する statement に帰着される。それを述べるのがこの目標である。

まず 2.1.5 で述べた A とは何かは，きりとせよう。$\rho : G_{\mathbb{Q},S} \longrightarrow GL_2(\mathbb{F}_\ell)$ は 2.1.1, 2.1.2 をみたす既約な表現とする。さらに ρ は modular であると仮定する。従って

3.1.1. $\quad \rho_A : G_{\mathbb{Q},S} \longrightarrow GL_2(A)$

なる modular form から来る表現で ρ_A を mod m_A したものが ρ となるものが存在する。ここに A は $\mathbb{Z}_p$ と finite な DVR で m_A はその極大 ideal, $\mathbb{F}_\ell$ が A の剰余体であるとする。ρ に対して一番適当な ρ_A を1つとり，これを fix する。そして deformation の条件 $(\mathcal{D})$ の中に 2.1.5 という条件を入れておくことにする。従って常に A-algebra 上の ρ の lifting を考えることになり，$R_{\mathcal{D}}$ も $T_{\mathcal{D}}$ も A-algebra となる。また $T_{\mathcal{D}}$ が modular な表現に関する universal deformation algebra であったことから

3.1.2. $\quad T_{\mathcal{D}} \xrightarrow{\alpha_A} A$

という環準同型で $\alpha_A \circ \rho_T = \rho_A$ となるものが存在する。次に 2.1.6 のて：$R_{\mathcal{D}} \longrightarrow T_{\mathcal{D}}$ と上の α_A を合成したものを β_A と書くことにする。

3.1.3 $\quad \beta_A : R_{\mathcal{D}} \xrightarrow{\tau} T_{\mathcal{D}} \xrightarrow{\alpha_A} A$

$$\mathfrak{p}_T = \ker(\alpha_A : T_{\mathfrak{D}} \longrightarrow A)$$

$$\mathfrak{p}_R = \ker(\beta_A : R_{\mathfrak{D}} \longrightarrow T_{\mathfrak{D}} \longrightarrow A)$$

とおく。$T_{\mathfrak{D}}$ は Gorenstein 環だから

$$T_{\mathfrak{D}} \simeq \mathrm{Hom}_A(T_{\mathfrak{D}}, A)$$

なる canonical でない同型が存在する。ここで

$$A \simeq \mathrm{Hom}_A(A, A) \xrightarrow[\hat{\alpha}_A]{} \mathrm{Hom}_A(T_{\mathfrak{D}}, A) \simeq T_{\mathfrak{D}}$$

(ここに $\hat{\alpha}_A$ は α_A の dual)

によって $1 \in A$ が $\eta \in T_{\mathfrak{D}}$ に写されるとする。このとき イデアル (η) は $\mathrm{Hom}_A(T_{\mathfrak{D}}, A) \simeq T_{\mathfrak{D}}$ のとりかたによらない。このとき次が成立する。

Theorem 3.1.4. $\#(\mathfrak{p}_R/\mathfrak{p}_R^2) \leq \#(A/\eta) < \infty$ であれば $R_{\mathfrak{D}} \twoheadrightarrow T_{\mathfrak{D}}$ は同型となる。

証明は可換代数である。

$$\#(\mathfrak{p}_R/\mathfrak{p}_R^2) \geqslant \#(\mathfrak{p}_T/\mathfrak{p}_T^2) \geqslant \#(A/\eta)$$

が成立することに注意して次の2つの命題を使えばよい。(ここで $\#(\mathfrak{p}_T/\mathfrak{p}_T^2) \geqslant \#(A/\eta)$ は Fitting ideal を使って示される。これは Mazur と Wiles が Iwasawa main conjecture を証明するときに key の部分で使った使いうと同じである。)

R, T は完備ネーター局所環, A-algebra とする。また $R \twoheadrightarrow T$, $T \twoheadrightarrow A$ なる全射が与えられているとし $\mathfrak{p}_T$, $\mathfrak{p}_R$ を上と同じように定義する。このとき

Proposition 3.1.5. T が A と locally complete intersection, $\mathfrak{p}_R/\mathfrak{p}_R^2 \simeq \mathfrak{p}_T/\mathfrak{p}_T^2$ が同型で, これが torsion A-module になっているとする。このとき $R \twoheadrightarrow T$ は同型。

T は Gorenstein であると仮定し、$\eta \in A$ を上と同様に定義する。

Proposition 3.1.6. $\mathfrak{p}_T/\mathfrak{p}_T^2$ が torsion A-module であるとする。このとき T が A 上 locally complete intersection であることと $\#(\mathfrak{p}_T/\mathfrak{p}_T^2) = \#(\mathcal{O}/\eta)$ は同値。

もとの状況にもどろう。Theorem 3.1.4 により すべては

3.1.7. $\#(\mathfrak{p}_R/\mathfrak{p}_R^2) \leq \#(A/\eta) < \infty$

の証明に帰着されたことになる。

Remark 3.1.8. $\rho_A : G_{\mathbb{Q},S} \longrightarrow GL_2(A)$ が $\mathbb{Q}$ 上の楕円曲線に対応する表現，つまり Tate module からできる表現であるとする。仮定からこの楕円曲線 E は modular で $\phi : X_0(N) \longrightarrow E$ なる parametrization が存在する。このとき定義から η なる A の元は $\deg \phi$ と思ってよい。

3.2. cohomology による解釈

$\mathrm{Ad}(\rho_A)$ を次のような $G_{\mathbb{Q},S}$ 加群とする。集合としては $M_2(A)$ (2行2列 A 係数行列全体)，$G_{\mathbb{Q},S}$ の作用は $\sigma(M) = \rho_A(\sigma) \cdot M \rho_A(\sigma)^{-1}$ で与えられるとする。deformation 理論 (cf. [M]) により，自然な単同型

3.2.1. $\mathrm{Hom}_A(\mathfrak{p}_R/\mathfrak{p}_R^2, K/A) \hookrightarrow H^1(G_{\mathbb{Q},S}, \mathrm{Ad}(\rho_A) \otimes K/A)$

が定義され，単射であることがわかる。ここに K は A の商体である。ここで

$$\mathrm{Ad}(\rho_A) \simeq \mathrm{End}(\rho_A, \rho_A) \simeq (\rho_A \otimes \rho_A)(-1) \simeq (\mathrm{Sym}^2 \rho_A)(-1) \oplus A$$

に注意する。ここに (-1) は Tate twist，A は Galois 群が

trivial に作用するものとする。従って問題は $\mathrm{Sym}^2\rho_A$ 係数の cohomology を調べることに帰着して行く。ここでついに zeta 関数との関係が現われるわけだが、そのために次の一般論を述べねばならない。

3.3. Bloch Kato 予想

予想について述べる前に 2.1. で述べた deformation data について訂正をしたい。我々は deformation data $(\mathcal{D})$ として 2.1.3 – 2.1.5 の他にそれに次の条件をつけ加える必要がある。

2.1.5 1/2 $\ell \in S \setminus \{p\}$ に対して $\psi|_{D_\ell} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}$ $\psi_1\psi_2 = \chi$

また最初に考えるのも 2.1.1, 2.1.2 以外に条件

2.1.2 1/2 $\ell \in S \setminus \{p\}$ に対して $\rho|_{D_\ell} \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$ $\chi_1\chi_2 = \chi$

I_ℓ (惰性群) 上で nonsplit

をつける。つまり条件 2.1.1, 2.1.2, 2.1.2 1/2 をみたす ρ に対して、2.1.3 – 2.1.5 1/2 をみたす ρ の持ち上げを考えその中で universal なものの環を $R_{\mathcal{D}}$, modular で universal なものを $\mathbb{T}$ とするのである。

さて 3.2.1 の写像の image を調べるために次のような群を定義する。A を上の通り $\mathbb{Z}_p$ 上 finite な完備離散付値環とする。T を $G_{\mathbb{Q}}$ が連続に作用する自由 A 加群とし、$V = T \otimes_A K$ (K は A の商体) とおく。このとき

$$H^1_f(\mathbb{Q}_\ell, V) := \ker(H^1(\mathbb{Q}_\ell, V) \longrightarrow H^1(\mathbb{Q}_{\ell,nr}, V)) \quad \ell \neq p$$
$$\ker(H^1(\mathbb{Q}_\ell, V) \longrightarrow H^1(\mathbb{Q}_\ell, V \otimes B_{cris})) \quad \ell = p$$

$$H^1_f(\mathbb{Q}_\ell, V \otimes K/A) := \mathrm{Im}(H^1_f(\mathbb{Q}_\ell, V) \to H^1(\mathbb{Q}_\ell, V \otimes K/A)) \quad \ell < \infty$$

$$H^1_{f\ Sp\mathbb{Z}}(\mathbb{Q}, V) := \ker(H^1(\mathbb{Q}, V) \longrightarrow \prod_{\ell<\infty} H^1(\mathbb{Q}_\ell, V)/H^1_f(\mathbb{Q}_\ell, V))$$

$$H^1_{f\ Sp\mathbb{Z}}(\mathbb{Q}, V \otimes K/A) := \ker(H^1(\mathbb{Q}, V \otimes K/A) \to \prod_{\ell<\infty} H^1(\mathbb{Q}_\ell, V \otimes K/A) / H^1_f(\mathbb{Q}_\ell, V \otimes K/A))$$

と定義する。ここに $\mathbb{Q}_{\ell,nr}$ は $\mathbb{Q}_\ell$ の最大不分岐拡大，つまり $\ell \neq p$ のときは $H^1_f(\mathbb{Q}_\ell, V)$ は Serre の cohomologie galoisienne における不分岐 cohomology（ℓ が good reduction prime である整数環上の etale cohomology で表される部分）であり，$\ell = p$ のときは Fontaine の p 進 period 環 B_{cris} を使って定義される群（$H^1_f(\mathbb{Q}_p, V)$ に入るかどうかは p 進 Hodge 理論の言葉で表される）である。上の定義の最後にある群 $H^1_{f,Spec\mathbb{Z}}(\mathbb{Q}, V\otimes K/A)$ を T あるいは V の Selmer 群とよび，$Sel(\mathbb{Q}, V\otimes K/A)$ と書くことにする。T が楕円曲線 E の Tate module のとき，$Sel(\mathbb{Q}, T_p(E)\otimes \mathbb{Q}_p/\mathbb{Z}_p)$ は有名な直峡の Selmer 群 $Sel(\mathbb{Q}, E_{p^n})$ に一致する。また $Ш(\mathbb{Q}, V\otimes K/A)$ を

$$Sel(\mathbb{Q}, V\otimes K/A) := H^1_{f\,Spec\mathbb{Z}}(\mathbb{Q}, V\otimes K/A)$$

$$Ш(\mathbb{Q}, V\otimes K/A) := Sel(\mathbb{Q}, V\otimes K/A) / Image\left(H^1_{f,Spec\mathbb{Z}}(\mathbb{Q}, V)\right)$$

で定義する。

さて 3.2.1 の写像を考えると，deformation についての条件 (※) から（$\rho_{univ}|_{D_\ell}$ の様子を見て）この写像の image は $Sel(\mathbb{Q}, Ad(\rho_A)\otimes K/A)$ に入る。$\ell = p$ のところでこれを示すには $H^1_f(\mathbb{Q}_p, Ad(\rho_A)\otimes K) = H^1_g(\mathbb{Q}_p, Ad(\rho_A)\otimes K)$ を使う。ここに geometric part H^1_g は一般に Galois 表現 V に対し，$H^1_g(\mathbb{Q}_p, V) = \ker(H^1(\mathbb{Q}_p, V) \to H^1(\mathbb{Q}_p, V\otimes B_{DR}))$ で定義される。そこで $Ad\rho_A \simeq (Sym^2\rho_A)(-1)\oplus A$ を考え $H^1_{f\,Spec\mathbb{Z}}(\mathbb{Q}, K/A)$ が trivial なことをあわせると 3.2.1 から

3.3.1. $$Hom_A(\rho_R/\rho_R^2, K/A) \hookrightarrow Sel(\mathbb{Q}, (Sym^2\rho_A)\otimes K/A(-1))$$

となる。

もう一度一般論にもどると，Bloch Kato 予想は motif に付う p 進表現 V に対し

$\#Ш(\mathbb{Q}, V\otimes K/A) =$ V の zeta 関数の特殊値を使って表される数

の型で述べられる。もちろん V の zeta 関数の特殊値には period とか regulator の項も現われる。つまりこの Bloch Kato 予想は Beilinson 予想を（mod 有理数をとずに zeta の

値を見るという点で）そうに精密化したものである。ここでは詳しくは述べないが，mod $\mathbb{Q}$ しるいたために，Ш のような有限群対象についての予想ができるのである。

さて $V = (\mathrm{Sym}^2 \rho_A)(-1) \otimes_A K$ としよう。このとき V の weight は 0 だから $H^1_{f\,\mathrm{Spec}\,\mathbb{Z}}(K, V) = 0$ も予想される。従って

$$\#\,Sel(\mathbb{Q}, V \otimes K/A) = \#\,Ш(\mathbb{Q}, V \otimes K/A)$$

も予想されるわけである。V の L 関数 $L(V, s)$ は $s = 0, 1$ が critical value だが，このとき保型形式の理論から $L(V, s)$ は解析接続と $s = 0, 1$ での値も計算されている。（有理数・period の型に書けている。）これと Bloch Kato 予想の式を比べることにより，このとき予想は

3.3.2. $$\#\,Sel(\mathbb{Q}, V \otimes K/A) = \#(A/\eta)$$

となることがわかる。一方我々が目標としている 3.1.7 は 3.3.1 から

3.3.3. $$\#\,Sel(\mathbb{Q}, V \otimes K/A) \leqq \#(A/\eta)$$

に帰着されることがわかる。そして 1 ページ目に述べた Wiles の言明にあった「Selmer 群の位数をある形と比べること」というのはこの 3.3.3. である。$\#(A/\eta)$ が 3.3.2 のように zeta の値から予想される数であることから，3.3.3 のような不等式は zeta の化身（= Euler system cf. 3.4）を使って証明されることが期待される。

$H^1_{f\,\mathrm{Spec}\,\mathbb{Z}}(\mathbb{Q}\ V \otimes K/A) = Sel(\mathbb{Q}, V \otimes K/A)$ の双対を Poincaré duality を頭において，$H^2(\mathrm{Spec}\,\mathbb{Z}, \mathrm{Sym}^2 \rho_A)$ とすることにする。

3.4. Kummer の仕事との対比

ideal 類群は上のように定義され一般化された Selmer 群の 1 つの例である。よく知られているように Kummer は Fermat 予想研究の途上で ideal 類群に出会

った，つまりやはり Selmer群に出会ったのである。
Riemann zeta を大事にする形で書くと，Kummer の扱ったのは "$H^2(\mathbb{Z}, \mathbb{Z}_p(r))$" $= H^2_{et}(\mathbb{Z}[\frac{1}{p}], \mathbb{Z}_p(r)) = H^2(G_{\mathbb{Q},\{p\}}, \mathbb{Z}_p(r))$
ここに r は $0 < r < p-1$ の偶数，である。H^1 で書きたければ $H^1(G_{\mathbb{Q},\{p\}}, \mathbb{Q}_p/\mathbb{Z}_p(r))$ で同じである。
$H^2(G_{\mathbb{Q},\{p\}}, \mathbb{Z}_p(r))$ の予想される位数は Riemann zeta 等を使って $\#(\mathbb{Z}_p/\zeta(1-r))$ と書ける。そして Kummer が彼の名のついている有名な criterion で示したのは，すべての 0 と $p-1$ の間の偶数 r で $p \nmid \zeta(1-r)$ であれば同じ範囲の r で $H^2(G_{\mathbb{Q},\{p\}}, \mathbb{Z}_p(r)) = 0$ である。またこの条件の下，この p に対して Fermat 予想が成立することを示した。そして最終的に

$$\# H^2(G_{\mathbb{Q},\{p\}}, \mathbb{Z}_p(r)) = \#(\mathbb{Z}_p/\zeta(1-r))$$

の式は Mazur と Wiles が Iwasawa Main Conjecture を証明したことで初めて示された。また最近の Kolyvagin の Euler system の議論によれば Gauss 和の Euler system を使って，(Iwasawa Main Conjecture は経由せずに)

$$\# H^2(G_{\mathbb{Q},\{p\}}, \mathbb{Z}_p(r)) \leqq \#(\mathbb{Z}_p/\zeta(1-r))$$

が言える。

Wiles の拡張にそうと，Kummer criterion にあたることは（ある条件の下）Flach [F] がやっている。彼は（ある条件の下）

(zeta 関数で予想される値)・Selmer群 $= 0$

を示した。方法は Euler system は作れるはずで Kolyvagin の方法であるとする。そこで Wiles は Euler system を構成することによって上の ideal 類群の場合のような不等式

#Selmer群 $(= \#"H^2(\mathbb{Z}, \mathrm{Sym}^2 \rho_A)")$ $\leqq$ (zeta 関数で予想される値)

を示そうとするのである。

3.5, Euler system

Wiles の Euler system については筆者にはほとんど語ることができない。論文も未発表であるし、前述のように一番難しいところでもあり、また system の構成には p 進 Hodge 理論に関する Faltings の定理が必要なのだが、その部分についても何かの噂がある。とにかくごくごく簡単なことしか書けない。

"$\#H^2(\mathrm{Spec}\,\mathbb{Z}, \mathrm{Sym}^2 \rho_A)$" を評価するために localization sequence

$$\to H^1(\mathbb{Q}, \mathrm{Sym}^2 \rho_A/p^N) \to \bigoplus_{\ell \in \mathrm{Spec}\,\mathbb{Z}} H^2_\ell(\mathrm{Spec}\,\mathbb{Z}, \mathrm{Sym}^2 \rho_A/p^N) \to H^2(\mathrm{Spec}\,\mathbb{Z}, \mathrm{Sym}^2 P/p^N)$$

を考える。$H^1(\mathbb{Q}, \mathrm{Sym}^2 \rho_A/p^N)$ に部分のいい元がいくつも作れれば、少なくとも $\bigoplus H^2_\ell(\mathrm{Spec}\,\mathbb{Z})$ からの image は小さくなる。Flach [F] は $H^1(\mathbb{Q}, \mathrm{Sym}^2 \rho_A/p^N)$ に次のようにえを作る。level Nl の modular form から $X = X_0(N) \times X_0(N)$ とおき $H^1(X, \mathbb{Z}_2)$ のえをうまく作り、$H^3(X, \mathbb{Z}/p^N(2))$ $H^1(\mathbb{Q}, H^2(X, \mathbb{Z}/p^N(2)))$, $H^1(\mathbb{Q}, \mathrm{Sym}^2 \rho_A/p^N)$ と持って来る。これを Euler system にするには abel 拡大が必要なのだが、Wiles は $X_1(N_0, N_1) \to X_0(N_0, N_1)$ という abel 拡大を使うという。以上のようにほとんどわからない状態なのでここで筆をおくことにしたい。

参考文献

[BK] Bloch and Kato, L-functions and Tamagawa numbers of motives, in "The Grothendieck Festschrift" Vol I (1990)

[F] Flach, M., A finiteness theorem for the symmetric square of an elliptic curve, Invent math 109 (1992)

[M] Mazur, B., Deforming Galois representations, in Galois groups over $\mathbb{Q}$, MSRI publications 16 (1989)

[R] Ribet, K., On modular representations of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, Invent math 100 (1990)

[S] Serre J-P., Sur les représentations modulaires de degré 2 de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, Duke Math 54 (1987)